VECTRA
SECURITY THAT THINKS.®

macmon
intelligent einfach

MACMON NAC WHITEPAPER

Integration von macmon NAC mit Vectra Cognito

nac

Integration von macmon NAC mit Vectra Cognito

Inhaltsverzeichnis

Version 1.3

1 Einleitung

Vectra ist ein weltweit führender Anbieter von KI zur Echtzeit-Erkennung und -Abwehr von Cyber-Angriffen in Cloud-, Rechenzentrums- und Unternehmensinfrastrukturen.

Dabei werden Security-Analysten bei der Durchführung schlüssiger Untersuchungen von Vorfällen und bei KI-gestütztem Threat- Hunting unterstützt. In heutigen schwierigen Datenumgebungen ist umfassende Erkennung und Response von Cyber-Angriffen unverzichtbar.

Vectra ist wie kein anderes Unternehmen in der Lage, Sie bei der proaktiven Suche nach Cyber-Angreifern und der Reduzierung des Geschäftsrisikos zu unterstützen.

Unser Kernteam besteht aus Bedrohungsforschern, White Hat-Hackern, Datenwissenschaftlern, Netzwerk-sicherheitsexperten und UI-Designern. Wir erweitern kontinuierlich die Grenzen des Möglichen, um die nächste Generation der Sicherheit noch besser zu machen.

2 Anwendungsfälle

2.1 macmon ruft bei Vectra Cognito die Risikoeinstufung der Endgeräte ab

Neben Viren und Schadsoftware kann einem Administrator auch verdächtiges Verhalten von Endgeräten das Leben schwer machen. Wenn eine solche schädliche Software trotz aller Vorsichtsmaßnahmen ein Endgerät infiziert, muss die Isolierung dieses Endgeräts aus dem Netzwerksegment so schnell wie möglich erfolgen. Dadurch wird verhindert, dass sich eine Schadsoftware über das Netzwerk verbreitet und andere im Netzwerk befindlichen Ressourcen infiziert. **Vectra Cognito** ist dank des Einsatzes von künstlicher Intelligenz in der Lage, eine solche Bedrohung schnell zu erkennen.

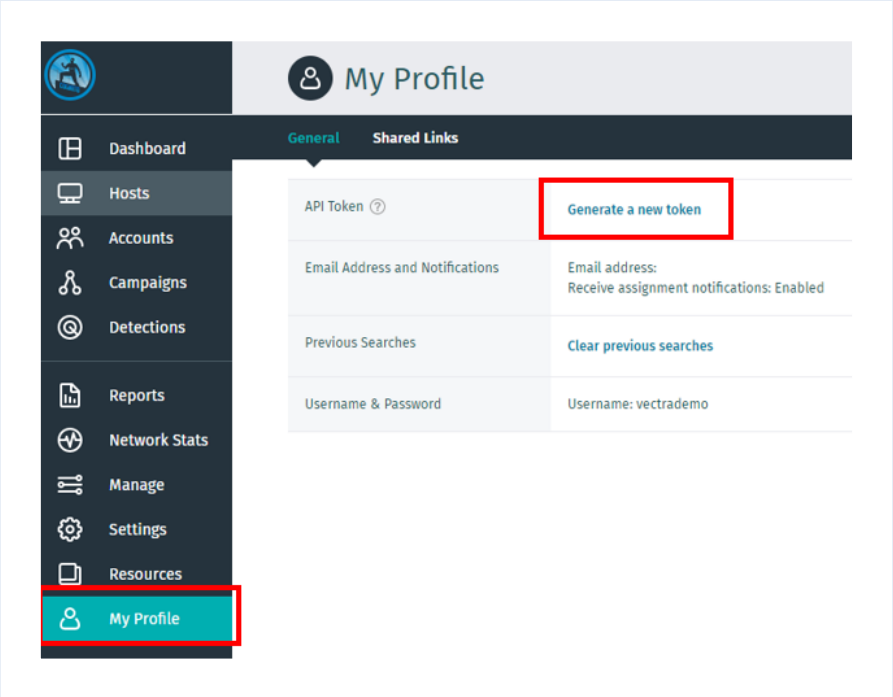
In **Vectra Cognito** wird der Systemzustand eines jeden Endgeräts im Unternehmensnetzwerk festgehalten und für **macmon NAC** bereitgestellt. Die Kombination aus **Vectra Cognito** und **macmon NAC** ist eine leistungsstarke Kombination aus Erkennung von Bedrohungen und Isolation von betroffenen Endgeräten.

Durch die bereitgestellten Informationen kann **macmon NAC** den Compliance-Status eines Endgeräts basierend auf der von **Vectra Cognito** festgestellten Risikoeinstufung des Endgerätes erzwingen. Dies gilt für Netzwerke jeglicher Größe, denn in jedem Netzwerk finden Sie Geräte, die möglicherweise Bedrohungen ausgesetzt sind. Wenn **Vectra Cognito** eine solche in Ihrem Netzwerk erkennt, klassifiziert sie die Bedrohungslage in die vier Zustände „niedrig“, „mittel“, „hoch“ und „kritisch“. Diese werden von **macmon NAC** regelmäßig ausgewertet und konfigurierbar verschiedenen Compliance-Status zugeordnet. Wird der Systemzustand „kritisch“ beispielsweise dem Compliance-Status „noncompliant“ zugeordnet, so sorgt eine voreingestellte Regel für die Isolation eines Endgeräts, indem es ins Remediation-VLAN verschoben oder der Netzwerkanschluss am Switch abgeschaltet wird.

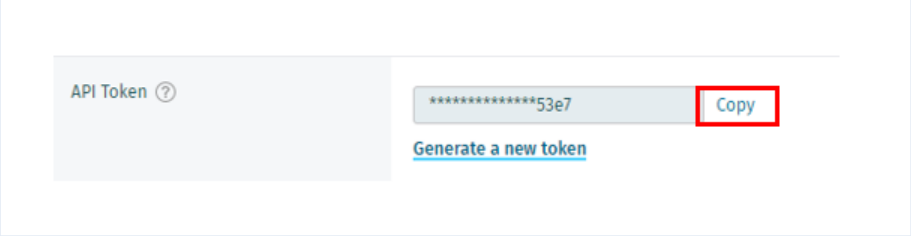
3 Konfiguration von Vectra Cognito

Im Folgenden werden die notwendigen Schritte zum Erstellen eines Tokens für den API-Zugriff durch **macmon NAC** beschrieben.

1. Tippen Sie auf *My Profile* und dort auf das Tab *General*. Tippen Sie danach auf *Generate a new token*.



Auf der folgenden Seite tippen Sie bei *API Token* auf *Copy*. Den Token benötigen Sie in Schritt 1 der Konfiguration von **macmon NAC**.

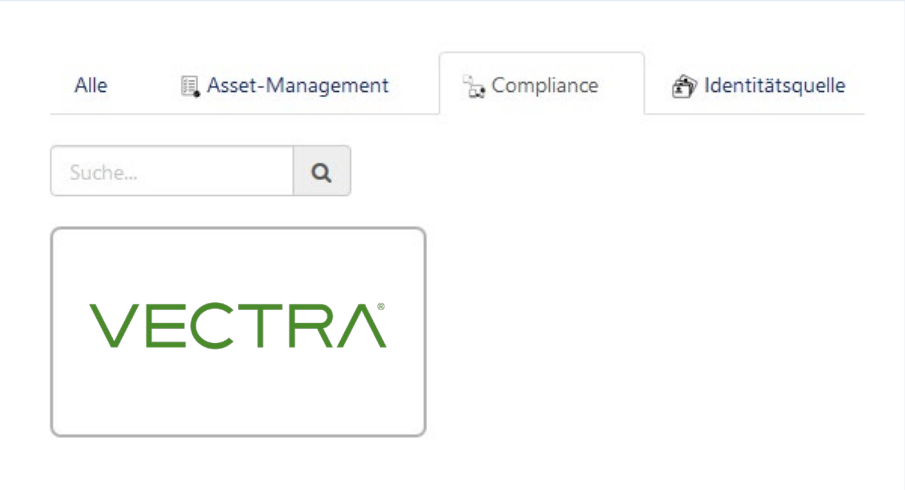


4 Konfiguration von macmon NAC

Im Folgenden wird beschrieben, wie die vorliegende Integration konfiguriert und aktiviert wird. Mit der Aktivierung wird ein Task in *Einstellungen → Geplante Tasks* angelegt, der im konfigurierten Intervall ausgeführt wird.

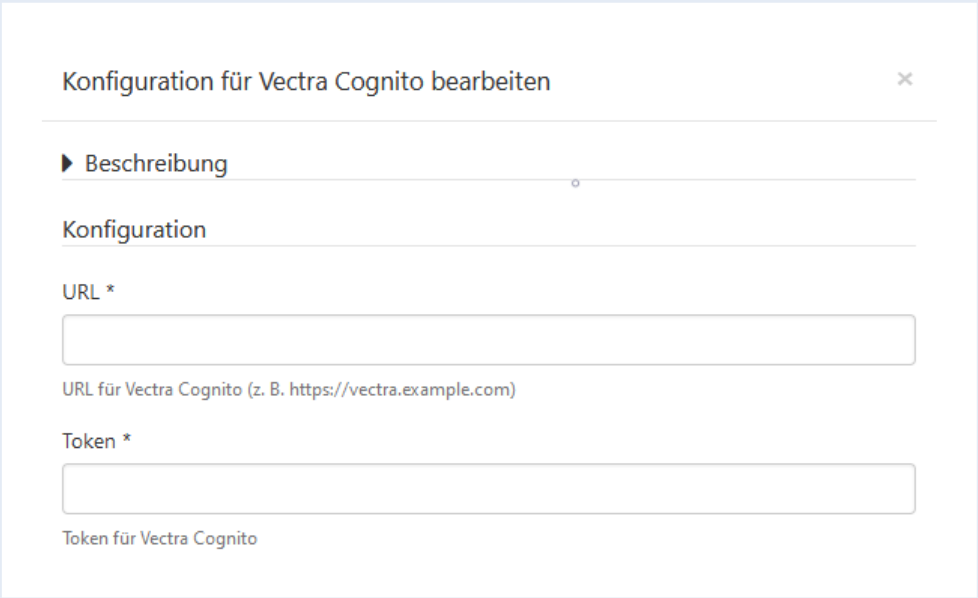
Eine Übersicht über alle abgefragten Endgeräte können Sie unter *Berichte → Endgeräte → Client Compliance* einsehen. Sie können dort nach der Quelle *Vectra Cognito* filtern.

Die Konfiguration wird über die Web-GUI vorgenommen. Wählen Sie dazu bitte *Einstellungen* und *Drittanbieter-Integrationen*, danach den Tab *Compliance*.



Wenn der Rahmen der **Vectra Cognito**-Kachel grau erscheint, ist die Integration noch nicht aktiviert. Bitte klicken Sie auf die Kachel, um den Konfigurationsdialog aufzurufen.

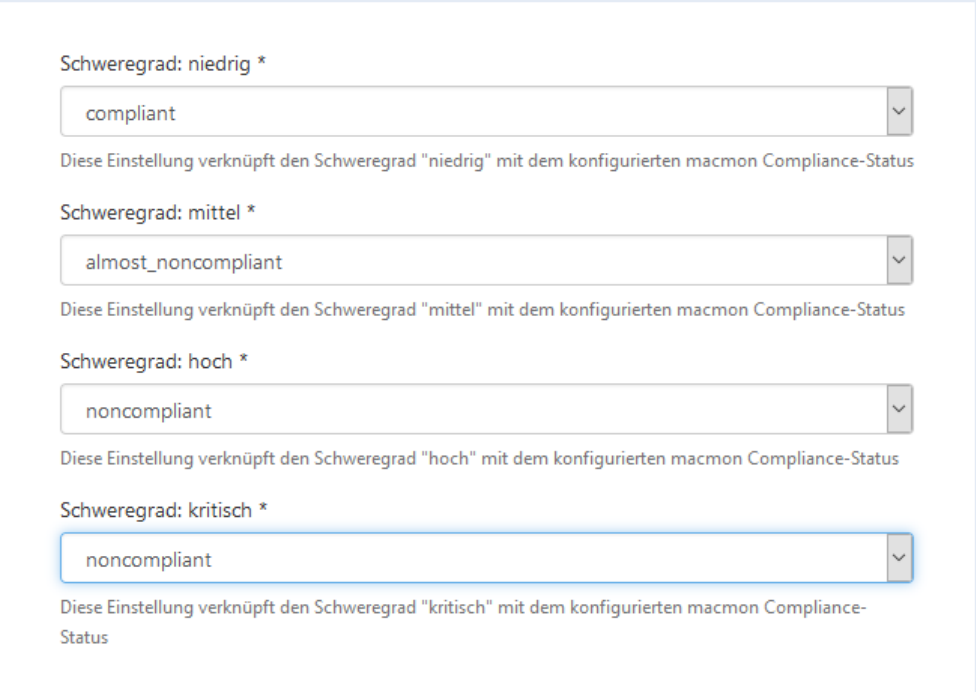
1. Geben Sie die URL ein, die notwendig ist, um die API von **Vectra Cognito** aufzurufen.
   Geben Sie außerdem den Token ein.



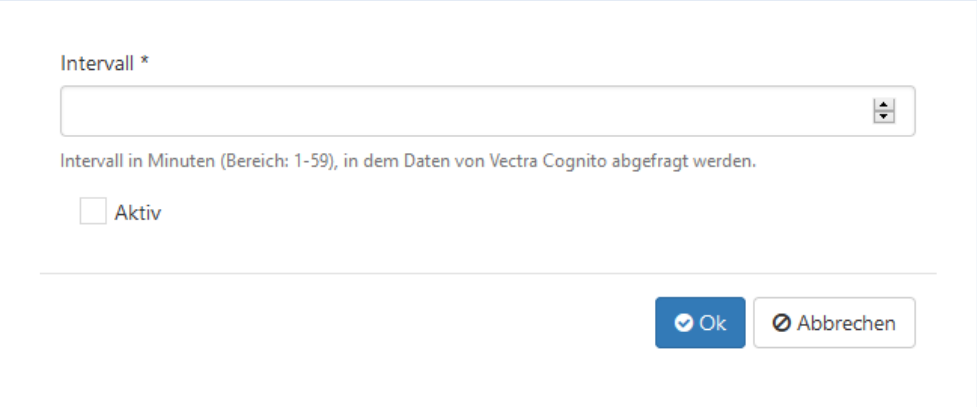
2. Setzen Sie den Haken bei Compliance, wenn der Compliance-Status gesetzt werden soll.
   Wählen Sie das Threat-Level und das Certainty-Level, nach welchen die Endgeräte gefiltert werden sollen um nur die Informationen zu Endgeräten ab einer gewissen Kritikalität einzuholen.

   Gemäß der Vectra Terminologie bezeichnet der Threat-Level dabei die Bedrohungsstärke und der Certainty-Level die Wahrscheinlichkeit einer Ausnutzung, wodurch im Verhältnis das Risiko errechnet wird.

3. Konfigurieren Sie, wie die verschiedenen Systemzustände in **macmon NAC** abgebildet werden sollen. Dies hat Auswirkungen auf das Setzen des Compliance-Status in **macmon** und der damit verbundenen Reaktion wie z.B. der Isolierung des entsprechenden Endgerätes.



4. Geben Sie das Intervall ein, in dem Daten abgerufen werden sollen.



5. Schließen Sie die Aktivierung mit Klick auf ***OK*** ab.

5 Unterstützte Versionen

macmon NAC, ab Version 5.33.1. mit der Lizenz **Premium Bundle**
Vectra Cognito, ab Version 6.1.0

Kontakt bei Vectra

Vectra Networks Germany GmbH
Elsenheimerstraße 7
80667 München

E-Mail: info_dach@vectra.ai

Kontakt

macmon secure GmbH
Alte Jakobstraße 79-80 | 10179 Berlin

Tel.: +49 (0) 30 23 25 777 – 0
nac@macmon.eu